Claims

1. A method for managing access to a device, said method comprising:

(a) sending a first message from a first device to a second device;

(b) receiving, in said first device, from said second device a digital certificate encrypted using a first private key of said second device;

(c) receiving, in said first device, from said second device said first message encrypted using a second private key of said second device;

(d) authenticating said second device in response to said digital certificate and said first encrypted message; and

(e) establishing a communication channel between said first and said second devices in response to the authentication of said second device.

2. The method of Claim 1 wherein said first message comprises first identification data associated with said first device and a date and time stamp.

3. The method of Claim 2 wherein said digital certificate comprises second identification data associated with said second device and a second public key of said second device.

4. The method of Claim 3 wherein the step of authenticating comprises the steps of:

(a) decrypting said digital certificate in said first device using a first public key;

(b) decrypting said first encrypted message using said second public key to generate a first decrypted message; and

(c) comparing said first decrypted message to said first message.

5. The method of Claim 4 wherein said first public key is stored in said first device.

6. The method of Claim 5 further comprising the step of providing confirmation of the authentication to said second device by

(a) encrypting said first message using said second public key to generate a second encrypted message; and

(b) sending said second encrypted message to said second device.

7. The method of Claim 6 wherein said digital certificate, said first public key and said first private key are issued by an independent certificate authority and are associated with said second device.

8. The method of Claim 1 wherein said first device is a set-top box and said second device is a server associated with a service provider.

9. The method of Claim 8 wherein said second identification data further comprises data associated with said certificate authority and data associated with the validity of said digital certificate.

10. A method for managing access to a device, said method comprising:

(a) sending first identification data associated with a first device to a second device;

(b) receiving, in said first device, from said second device a digital certificate encrypted using a first private key of said second device, said digital certificate having second identification data associated with said second device and a second public key of said second device;

(c) encrypting said first identification data in said second device using a second private key associated with said second device to generate first encrypted identification data;

(d) receiving, in said first device, from said second device said first encrypted identification data;

(e) decrypting in said first device, using a first public key to obtain said second public key, said encrypted digital certificate received from said second device, said first public key being stored in said first device;

(f) decrypting said first encrypted identification data using said second public key to generate a first decrypted identification data;

(g) authenticating said second device by comparing said first decrypted identification data to said first identification data;

(h) sending to said second device second encrypted identification data, said second encrypted identification data being encrypted in said first device using said second public key of said second device; and

(i) establishing a communication channel between said first and said second devices.

11. A system for managing access between a service provider and a set-top box having a smart card coupled thereto, said set-top box performing the steps of:

(a) sending a first message to the smart card, said first message containing set-top box identification data;

(b) receiving from the smart card, in response to said first message, a first digital certificate encrypted using a first private key, said first digital certificate containing service provider identification data;

(c) authenticating the smart card in response to said first digital certificate;

(d) contacting the service provider in response to the authentication of the smart card and said service provider identification data and sending a second message to the service provider, said second message containing set-top box identification data;

(e) receiving from the service provider, in response to said second message, a second digital certificate encrypted using a second private key of said service provider;

(f) receiving from the service provider said second message encrypted using a third private key;

(g) authenticating the service provider in response to said second digital certificate and said second encrypted message;

(h) providing confirmation of the authentication to the service provider; and

(i) establishing a communication channel with the service provider in response to the authenticated service provider.

12. The system of Claim 11 wherein the smart card comprises a plurality of digital certificates, each one containing service provider identification data associated with a unique service provider.

13. The system of Claim 12 wherein the step of authenticating the smart card in response to said first digital certificate comprises decrypting said first digital certificate in said set-top box using a first public key.

14. The system of Claim 13 wherein said second digital certificate comprises second service provider identification data and a second public key of said service provider.

15. The system of Claim 14 wherein the step of authenticating the service provider comprises the steps of:

(a) decrypting said second digital certificate in the set-top box using said second public key;

(b) decrypting said encrypted second message using a third public key to generate a second decrypted message; and

(c) comparing said second decrypted message to said second message.

16. The system of Claim 15 wherein said first public key, said second public key, said first message and said second message are stored in said set-top box.

17. The system of Claim 16 wherein said first digital certificate, said first private key and said first public key are issued by an independent certificate authority.

18. The system of Claim 17 wherein said first digital certificate is stored in said smart card.

19. The system of Claim 18 wherein said second digital certificate, said second private key and said second public key are issued by an independent certificate authority and are associated with said service provider.

20. The system of Claim 19 wherein said second digital certificate is stored in said service provider.